Attorney Docket No: 40116/03701 (1546)

IN THE CLAIMS:

Please amend the claims as follows:

1. (Currently Amended) A method for establishing an authenticated wireless communication between a first mobile device and a second device, comprising the steps of:

sending an initial signal by the first device to establish a wireless communication with the second device, the first device including only a data capturing arrangement ("DCA") as an input device interface with a user thereof;

initiating an authentication process by the second device;

obtaining a PIN code from the user via the DCA, ~~the PIN code being obtained by the DCA,~~ the PIN code identifying at least one device with which the first device is authorized to communicate ~~indicates an identity of the second device to the first device~~;

performing a pairing process to compare the PIN code to entries in a database of authorized PIN codes;

when the pairing process has been successfully completed, generating a link key to establish the authenticated wireless communication between the first and second devices.

2. (Original) The method according to claim 1, wherein the databases is stored in a memory arrangement of the second device.

3. (Original) The method according to claim 1, wherein the first device is a mobile barcode scanner.

4. (Original) The method according to claim 1, wherein the first device communicates with the second device using Bluetooth technology.

5. (Original) The method according to claim 1, wherein the obtaining step further includes the following substeps:

scanning a barcode using the DCA, the barcode being provided by the user as the PIN code, and

converting the barcode into the PIN code using a processor of the first device.

6. (Original) The method according to claim 1, wherein the second device includes a wireless access point which communicates with the first device.

7. (Original) The method according to claim 1, wherein the first device includes an alerting arrangement notifying the user when to enter the PIN code.

8. (Original) The method according to claim 7, wherein the alerting arrangement includes at least one of a speaker emitting a predetermined sound and a set of LEDs emitting a predetermined lighting pattern.

9. (Original) The method according to claim 1, wherein the obtaining step includes the following substeps:

limiting a time period for the user to enter the PIN code to a predetermined time period, and

refusing to accept the PIN code from the user when the predetermined time period has expired.

10. (Currently Amended) The method according to claim 1, wherein the pairing process includes the following substeps:

compiling a ~~providing~~ first sample data, from a collection of random data, by the second device, the second device then providing the first sample data to the first device,

generating second data, by the first device, as a function of the first sample data, the PIN

code and a hashing procedure;

providing at least a portion of the second data by the first device to the second device,

generating third data by the second device as a function of at least one of the authorized PIN codes stored in the database, the second data received from the first device and the hashing procedure;

comparing, by the second device, the second data received from the first device to the corresponding third data ~~by the second device~~, and

when the second data received from the first device matches to the third data, generating an indication the pairing process is successfully completed.

11. (Original) The method according to claim 1, wherein the link key is one of a temporary key which is effective only for a single session and a long-term key which is effective for multiple sessions between the first and second devices.

12. (Original) The method according to claim 1, further comprising the step of:

establishing a secure communication between the first and second devices using a predetermined encryption technology.

13. (Currently Amended) A system for establishing an authenticated wireless communication, comprising:

a first wireless mobile device including only a data capturing arrangement ("DCA") as an input device interface with a user thereof; and

a second device receiving an initial signal from the first device to establish a wireless communication, the second device initiating an authentication process,

wherein the first device obtains a PIN code from the user via the DCA, ~~the PIN code being obtained by the DCA,~~ the PIN code identifying at least one device with which the first device is authorized to communicate, ~~indicates an identity of the first device to the second device,~~ wherein the first and second devices perform a pairing process to compare the PIN code

to entries in a database of authorized PIN codes, and wherein, when the pairing process has been successfully completed, the first and second devices generate a link key to establish the authenticated wireless communication.

14. (Original) The system according to claim 13, wherein the second device includes a memory arrangement storing the database.

15. (Original) The system according to claim 13, wherein the first device is a mobile barcode scanner.

16. (Original) The system according to claim 13, wherein the first device communicates with the second device using Bluetooth technology.

17. (Original) The system according to claim 13, wherein the first device scans a barcode using the DCA, the barcode being provided by the user as the PIN code, a processor of the first device converting the barcode into the PIN code.

18. (Original) The system according to claim 13, wherein the second device includes a wireless access point which communicates with the first device.

19. (Original) The system according to claim 13, wherein the first device includes an alerting arrangement notifying the user to enter the PIN code.

20. (Original) The system according to claim 19, wherein the alerting arrangement includes at least one of a speaker emitting a predetermined sound and a set of LEDs emitting a light in a predetermined lighting patterns.

21. (Currently Amended) The system according to claim 13, wherein the pairing process

includes the following substeps:

compiling a ~~providing~~ first sample data, from a collection of random data, by the second device, the second device then providing the first sample data to the first device,

generating second data, by the first device, as a function of the first sample data, the PIN code and a hashing procedure;

providing at least a portion of the second data by the first device to the second device,

generating third data by the second device as a function of at least one of the authorized PIN codes stored in the database, the second data received from the first device and the hashing procedure;

comparing, by the second device, the second data received from the first device to the corresponding third data ~~by the second device~~, and

when the second data received from the first device matches to the third data, generating an indication the pairing process is successfully completed.

22. (Original) The system according to claim 15, wherein the link key is one of a temporary key which is effective only for a single session and a long-term key which is effective for multiple sessions between the first and second devices.

23. (Original) The system according to claim 13, wherein the first and second devices establish a secure communication using a predetermined encryption technology.

24. (Currently Amended) A wireless mobile device for establishing an authenticated wireless communication with a further device, comprising:

a processor;

a wireless communication arrangement; and

a data capturing arrangement ("DCA") being the only input device interface for a user thereof,

wherein the processor generates a request for establishing an authenticated wireless

communication, the request being forwarded to the further device via the communication arrangement, the communication arrangement receives from the further device a first sample data, compiled from a collection of random data, and a request for second data, the DCA obtaining a PIN code from the user, ~~the PIN code being obtained by the DCA,~~ the PIN code ~~indicates an identity of the wireless mobile device to the further device~~ identifying at least one device with which the mobile device is authorized to communicate, the processor generating the second data as a function of the PIN code, the first sample data and the hashing procedure, the second data being provided, by the mobile device, to the further device,

wherein the further device generates third data as a function of at least one of the authorized PIN codes stored in a database, the second data received from the mobile device and the hashing procedure, and

wherein, when the second data received from the mobile device matches ~~matched~~ to the third data, the mobile device and the further device generate a link key to establish the authenticated wireless communication.

25. (Currently Amended) The mobile device according to claim 24, wherein the mobile device is a mobile barcode scanner.

26. (Currently Amended) The mobile device according to claim 24, wherein the mobile device communicates with the further device using Bluetooth technology.

27. (Currently Amended) The mobile device according to claim 24, wherein the DCA scans a barcode which is provided by the user as the PIN code, the processor converting the barcode into the PIN code.

28. (Currently Amended) The mobile device according to claim 24, further comprising:

an alerting arrangement notifying the user to enter the PIN code.

29. (Currently Amended) The mobile device according to claim 24, wherein the alerting arrangement includes at least one of a speaker emitting a predetermined sound and a set of LEDs emitting a predetermined lighting pattern.